Pers Ubiquit Comput (2016) 20:875–884
DOI 10.1007/s00779-016-0966-0

ORIGINAL ARTICLE

Android platform-based individual privacy information protection system

Weizhe Zhang[1] · Xiong Li[1] · Naixue Xiong[2] · Athanasios V. Vasilakos[3]

Received: 31 January 2016 / Accepted: 29 July 2016 / Published online: 16 September 2016

Abstract With the popularity of mobile phones with Android platform, Android platform-based individual privacy information protection has been paid more attention to. In consideration of individual privacy information problem after mobile phones are lost, this paper tried to use SMS for remote control of mobile phones and providing comprehensive individual information protection method for users and completed a mobile terminal system with self-protection characteristics. This system is free from the support of the server and it can provide individual information protection for users by the most basic SMS function, which is an innovation of the system. Moreover, the protection mechanism of the redundancy process, trusted number mechanism and SIM card detection mechanism are the innovations of this system. Through functional tests and performance tests, the system could satisfy user functional and non-functional requirements, with stable operation and high task execution efficiency.

Keywords Android · Information security · Mobile device · Remote control · SMS message

✉ Weizhe Zhang
wzzhang@hit.edu.cn

Naixue Xiong
neal.xiong@swosu.edu

Athanasios V. Vasilakos
vasilako@ath.forthnet.gr

[1] School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China

[2] Department of Business and Computer Science, Southwestern Oklahoma State University, Oklahoma, OK, USA

[3] Lulea University of Technology, Luleå, Sweden

1 Introduction

After Google released Android 1.0 intelligent moving platform in 2008, Android quickly replaced Symbian with its unique open-source advantage and stood up to iPhone as an equal in mobile phone industry. Mobile phone manufacturers competed to bring out mobile phones with Android platform and presented the market trend of demand exceeding supply. Nowadays, more and more people are using mobile phones with Android platform, with a growth of tens of thousands in China, especially the young consumer group chasing for fashion.

People can download Android for free and bring convenience and fun to their life. However, they may intentionally or unintentionally save their private information in mobile phones. With the higher intellectualization degree of mobile phones, this phenomenon tends to be universal and more and more users tend to save their private information on mobile phones, because it is more convenient and private compared with PC. Therefore, casual privacy protection of mobile phones may bring unknown risks to people [1].

1.1 Motivation

It is often to see in life that you find your mobile phone left at home when you work; or in office after you return home from work; or in the dormitory when you are in classroom. Even worse, you may find it lost. In these circumstances, not only is the mobile phone not available for use but also you will be worried about the confidentiality of privacies in mobile phones.

Nowadays, most protection software or measures of mobile phones with Android platforms (including screen design unlocking and password unlocking) hinder the

normal use of mobile phones to some extent. Thus, to ensure the normal and smooth use of mobile phones, users choose to close these procedures or measures. Furthermore, once mobile phones are not available, lost or stolen, it is too late to take safety measures. When mobile phones are lost, the privacy information in them is more important. Once contact information, SMS contents and data information in SD card are used by illegal people, the consequences will be hard to imagine.

This system is devoted to providing comprehensive privacy information protection measures with strong practicability in case of unavailable mobile phones for mobile phone users with Android platform. It utilizes the most basic SMS function to provide these protection measures without influencing the normal use of mobile phones.

At the same time, considering the lack of current mobile phone information protection software and measures, this paper started from the view point of users to complete some innovative work for better application of this system and mobile phones by users, for example, self-protection function, mode switch, setting trusted number and password recovery. The system considers the safety of user data as much as possible to prevent information leakage.

Our main contributions are threefold:

1. We design and implement a system for Android-based mobile phone privacy information protection. This system is free from the support of the server, and it can provide individual information protection for users by the most basic SMS function.
2. We have the following innovations about the protection mechanism of the redundancy process, trusted number mechanism and SIM card detection mechanism.
3. We evaluate our optimized solution in a real environment with 150 real phones. It is found that the start-up time is within 2 s, CPU and memory occupation are reasonable, the mean of SMS task execution time is less than 4 min and the flow of 200 contact backing up is about 10 k.

Section 2 states some related works; Sect. 3 puts forward the Android platform-based individual privacy information protection system architecture and the key execution techniques; Sect. 4 illustrates the test and analysis of the system performance; and Sect. 5 provides the conclusion.

2 Related Works

Android platform has developed rapidly with its unique openness advantage. In smart phone platforms, the protection of users' privacy information has always been a hot topic. Different research and development groups strengthen their advantages and propose their mobile phone information protection measures. In general, for current Android platforms, the mobile phone information protection software is mainly divided into the following categories.

1. Screen locking [2], which covers password screen locking and gesture screen locking. The principle is to preset the mobile phone entering command and every time mobile phones are turned on, they need password detection, which can prevent unauthorized mobile phone invasion. The disadvantage is inconvenience. This kind of protection measure may hinder the normal use of mobile phones and leak the user privacy information.
2. System security [3], which owns various functions and provides virus scanning [4–8], file detection [9–12], anti-harassment of calls and messages for mobile phones. Its feature is various functions, but it occupies too many system resources, which decreases the usability of mobile phones. It does not belong to the same range of this study. Moreover, the reliability of this kind of procedure is extremely low and it is easy to leak user privacy information [13].
3. App protector, whose principle is based on utilizing the common application programs to save privacy information of users. When some procedures are launched, command verification can be made to protect user privacy information. Its drawback is the same as screen locking, hindering the normal use of mobile phones [14].

The above three kinds of information protection programs all have good application, and most mobile phones usually use one or more of them [15–19]. Also, a location-assisted Wi-Fi discovery scheme [20] is proposed to allow the user to switch to the Wi-Fi interface intelligently. Our former work also designed a system to detect bad information in mobile wireless networks based on the wireless application protocol [21] and protect user privacy on the Android-based mobile platform [22].

However, these methods all have the following shortcomings.

1. The protection measures must be preset. Once mobile phones are lost, no emergency plan can be made.
2. They are very fragile and all can be directly forbidden or uninstalled.
3. For lack of effective password management mechanism, once users forget password or command, it will be troublesome.
4. They reduce the mobile phone use efficiency, or hinder the normal use of mobile phones or occupy too many

system resources. Users usually will forbid these protection measures.

3 Framework of the Android platform-based individual privacy protection system

This system is divided into foreground interface, background program and data processing. Users can execute the corresponding functions in foreground interface, for example, mode switch, information modification, contact backup and recovery and password recovery. Background program mainly includes four subsystems, respectively, SMS processing subsystem, mobile phone locking subsystem, task management subsystem and self-protection subsystem. Data processing system mainly is in charge of operations relevant to data.

The system architecture is shown in Fig. 1. The interaction body between foreground interface and background program is function. Foreground interface is to execute some specific functions, for example, mode switch, information modification, contact backup and recovery, password recovery, sending e-mail, turning-on and turning-off of network connections. Task management subsystem is for the management of background tasks, including task execution, task duplication removal, task configuration information control and task interrupt recovery; SMS processing subsystem is responsible for the relevant processing of messages, including SMS monitoring, SMS reading and sending. Maintenance subsystem is in charge of operating conditions of the system in equipment, including the system start-up and continuous operation of the system after starting up; mobile phone locking subsystem is for locking mobile phones to prevent illegal use of mobile phones, including showing owner information, showing screen locking reasons, password recovery, contact the owner, receiving phone calls and unlocking; defense subsystem is for self-protection of the system, dealing with the malicious damage of the outside world to the system, including mandatory stop, clearing data and uninstallation.

Remote mobile phones can interact with the system by sending SMS and execute the corresponding commands by containing password, for example, locking, backing up and formatting. When backing up contact information, the system needs sending data by network connections and contact information data are sent to mail servers. When obtaining the current location information, network connections and location-based service provider are utilized for data transmission, sending location acquisition request and receiving location information.

3.1 SMS processing subsystem

This subsystem is to process operations relevant to SMS. One of the core functions of the system is to remote control mobile phones by SMS. Thus, SMS processing module plays an important role in the system. This module is divided into three submodules, SMS intercept module, SMS sending module and SMS reading module.

3.1.1 Formats of SMS commands

The system continuously background monitors SMS. Once receiving a piece of SMS, the head of this SMS is read. If this message conforms to the format of this system, this SMS will be intercepted. Thus, the focus of SMS processing subsystem is to design a set of SMS command formats of this system. Formats of SMS commands in this system are designed in Fig. 2.

First, if it is started with @pp, the head field of the command, it means this system needs to process this SMS. Then, it is followed by password field, which requires users to input locking codes. Next is operator field, which contains the corresponding operators of to-be-executed functions. The remote operations supported by the system include screen locking, contact backing up, contact deleting, call record deleting, SMS deleting, data of SD card deleting, displaying specific information on the lock screen, obtaining the current location of mobile phones and asking for password. Among them, deleting and asking for password can only be executed by sending SMS of trusted numbers. These operations are executed by remote control of common SMS, without other data transmission.

3.1.2 SMS monitoring module

The work flow of SMS monitoring is, SMS arriving—system sending broadcast—this system reading SMS content—if SMS conforms to specific format, reading SMS and judging whether the locking password in it is accurate. If it is accurate, call SMS intercept module to intercept the messages, save the number that sends SMS and operators, and call task management subsystem to execute the corresponding commands. After the execution is over, return to the executed results by SMS. Otherwise, no processing is made and the right of broadcast possession is released to let other broadcast receivers process.

In Android platform, when mobile phones receive SMS, the system will broadcast its arrival, with broadcast type of Telephony.SMS_RECEIVED. Thus, broadcast receiver of SMS_RECEIVED is used to obtain the arrival information of SMS. If this SMS conforms to the format of this system, it will directly intercept it instead of displaying it.

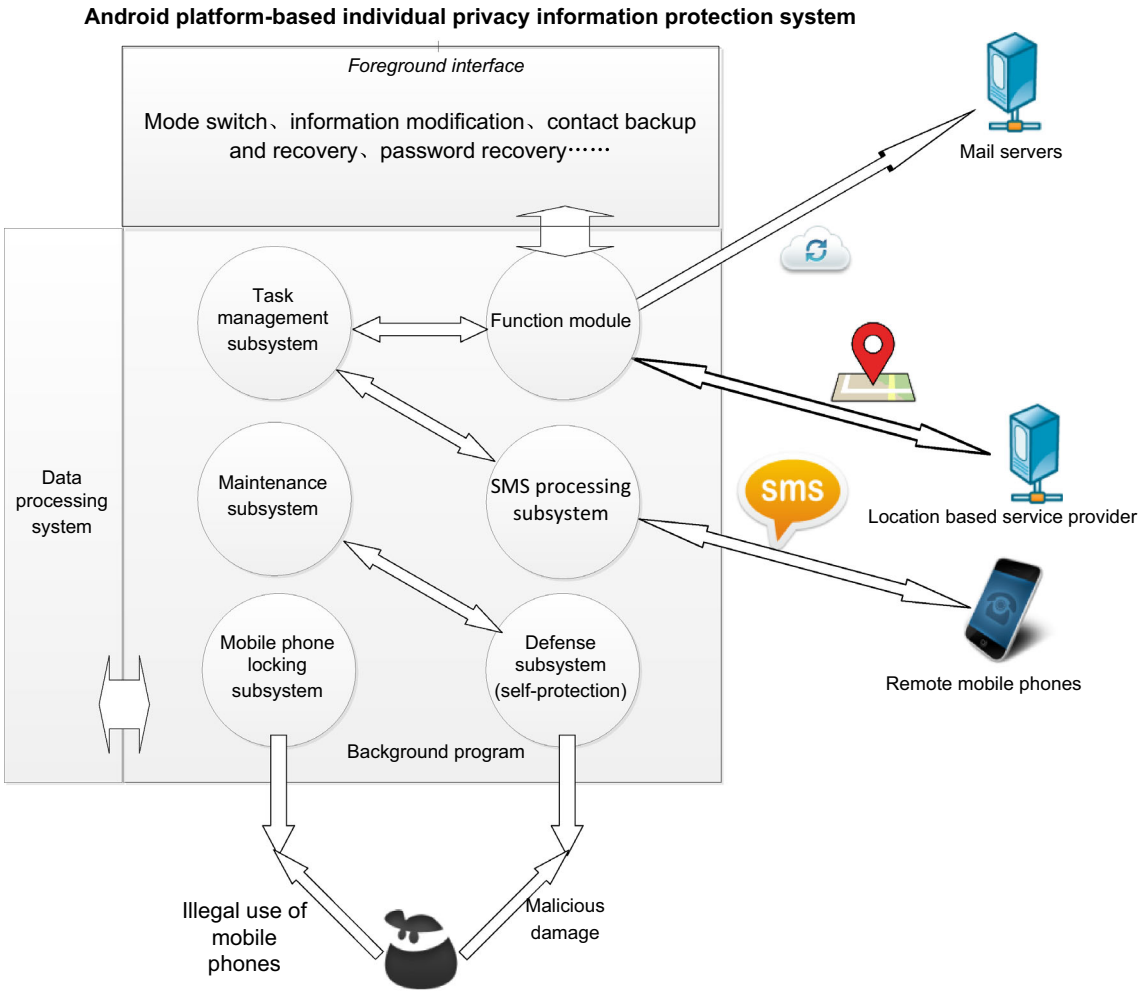


Fig. 1 Overall architecture of Android platform-based individual privacy protection system

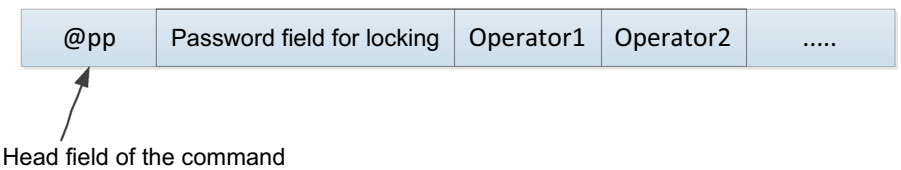


Fig. 2 Structure drawing of formats of SMS commands

However, many other SMS applications on Android platform (for example, message) and SMS applications developed by other manufacturers own monitoring functions. Therefore, to realize the SMS intercept, the priority of broadcast receiver in this system to SMS received shall be higher than other applications. The highest priority of broadcast in Android system is defined as 1000.

3.1.3 SMS reading module

First, the whole SMS content is read in internal storage as character string. Because the content of each SMS shall be no more than 70 characters, the content of one SMS can be divided to several to be delivered. Thus, these SMSs need to be collected as whole information. After obtaining the whole information, string operations are made and each section of information is, respectively, obtained according to the separator of information fields.

3.1.4 SMS intercept module

When SMS format conforms to the format defined in this system and the locking password in SMS is accurate, this SMS shall be intercepted to prevent other SMS applications from obtaining the information in this SMS, which can be realized through broadcast termination, namely

terminating the broadcast of current SMS arrival. In this way, other applications do not perceive this SMS broadcast, so they think there is no SMS arrival. This is the layer mechanism of Android-based broadcast receiver, which means receivers with higher priority can obtain broadcast information earlier than those with lower priority. Using broadcast termination to intercept SMS requires that the priority of SMS broadcast receiver be the highest globally. Through abortBroadcast(), continuous sending of SMS broadcast is terminated.

3.1.5 SMS sending module

When sending SMS, the content of SMS shall be obtained firstly, as well as the receiving number. Because service providers stipulate that the content of each SMS shall be no more than 70 characters, it is necessary to judge whether SMS is more than the upper limit. If so, there are two solutions. One is to segment the content and send in several pieces and the other one is to convert SMS into MMS (Multiple Message Service), which charges service charges for each MMS. Thus, this system adopted the latter one for greater text information.

If mobile phones work normally, SmsManager in Android is used to send SMS. According to the returned results, the sending state of SMS is judged.

3.2 Screen locking subsystem

Mobile phone screen locking is one core module in this system. Once mobile phones enter into lock screen, it can prevent others from operating them. The completion of the lock screen system consists of four parts, full screen anti-entering, displaying owner information, displaying reasons for screen locking, password recovery, contacting owners, answering an incoming call and unlocking module.

3.2.1 Full screen anti-entering module

In Android SDK, there is direct API of lock screen. Thus, the lock screen of this system shall be manually constructed. In typical Android mobile phones, user interactive components include notification bar, home screen and keyboard. The screen methods for each interactive component are shown in Table 1.

The key to full screen anti-entering lies in the construction of full screen interface. There is no method to release the interface unless automatic release, namely cut off and restart. It can screen notification bar and keyboard of Android mobile phones. On this interface, there is display space for displaying reasons for screen locking, displaying owner information, contacting owners, password recovery, answering an incoming call and unlocking module.

Table 1 Interactive components of Android mobile phones and their screen methods

Interactive components	Screen methods
Home screen	Display lock screen
Notification bar	Full screen display
Keyboard	Screen keyboard

3.2.2 Contacting owners and answering an incoming call

Contacting owners mainly obtain the current number of owners, which is determined by the sending number when the screen locking subsystem is called. Then, the mutual call and call-by-value mechanism between Android Activity components shall be obtained to open the Activity of call in background, introducing the number and realizing calls. However, directly calling Activity of call may cause thread blocking. Thus, a new thread shall be opened and multi-thread technology is utilized to avoid blocking.

When answering calls, Android operating system will send the system broadcast of android.intent.action. PHONE_STATE, so one broadcast receiver is registered when establishing the lock screen interface. In this receiver, the current dialing state is judged, which can be realized by Telephone Manager. Its getCallState() method can obtain the current dialing state. Monitoring calls is the first step and then buttons shall be displayed and the call shall be answered. The flow of answering calls is displaying a button of answering calls, clicking the button, telephone connection and button disappearing of call hang-up.

3.2.3 Unlocking module

If users input correct passwords, the lock screen can be released. The unlocking module not only needs unlocking passwords, but also needs to execute some cleanup.

Cleanup is to delete the established data or recover the modified configuration information. First, the interface with type of SYSTEM_ERROR needs to be removed, which needs to be realized by Window Manager object. Later, the system configuration information needs to be modified, changing whether locking configuration item into unlocked, representing that the system is in unlocked state. The registered call broadcast receiver when the locking interface is established shall be logged out. When the locking interface is established, the lock screen of Android system shall be turned off (using disable() of

KeyguardManager); while when unlock screed, the lock screen of the system shall be recovered.

3.3 Task management subsystem

Task management subsystem is the background engine of the system remote control function. It is in charge of managing task duplication removal, distribution, execution and configuration. Moreover, it is easy to interrupt when it works on mobile equipment (for example, power off or power down). Thus, it needs to realize the interrupt recovery of task execution.

When one or more SMS commands arrive, SMS processing system identifies these commands and transmits them to task management subsystem. This subsystem needs to have task identification and duplication removal and then, respectively, distribute tasks to these commands and carry out task configuration. The function of task execution comes from function module. After the task is executed, return to task execution results. When all tasks are completed, this subsystem summarizes the task execution results and distributes to each command and call SMS subsystem, returning to results in form of sending SMS. The design principle of this module is shown in Fig. 3.

In the process of task execution, in case of interruption, task interrupt recovery mechanism is introduced. Before task execution, task information is firstly saved, including the attribute that whether the task is completed. Then, it executes. After the execution is over, the task information

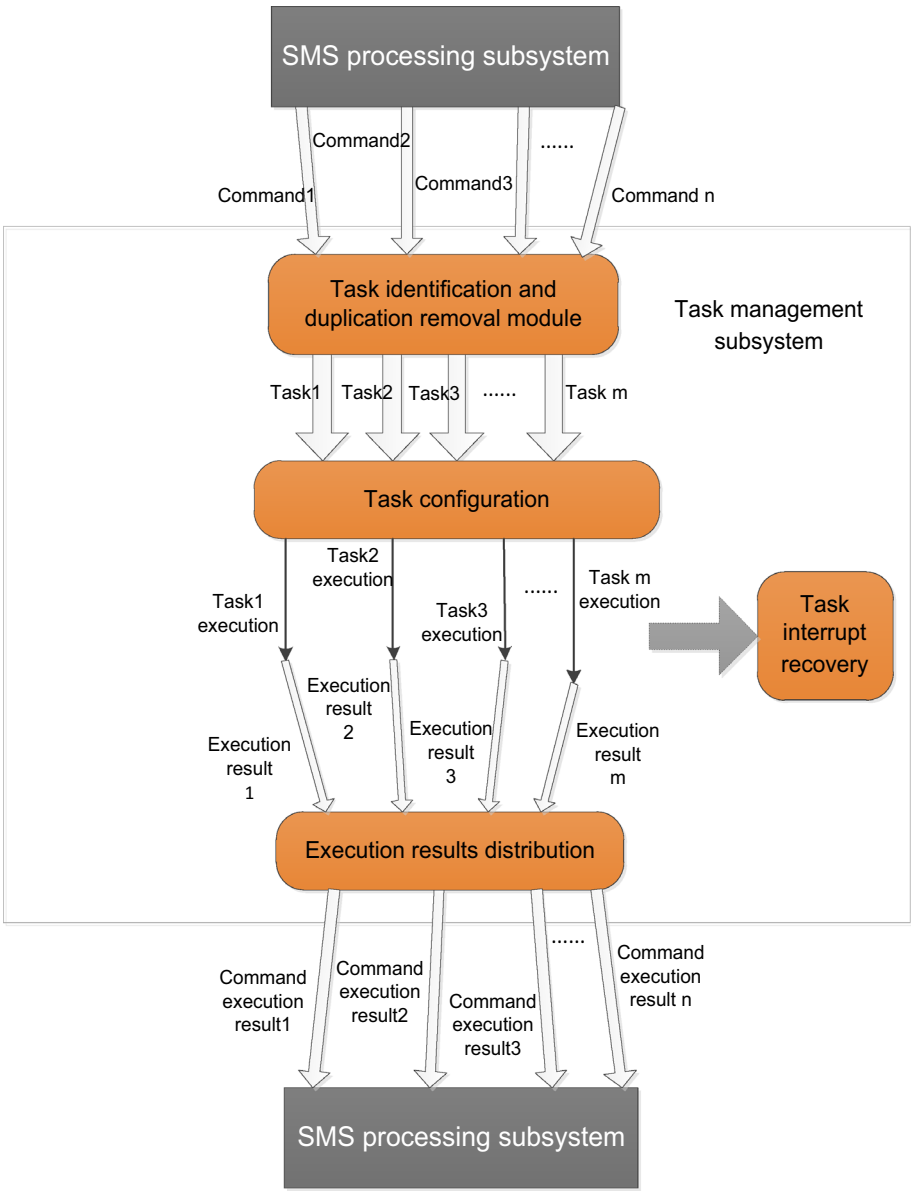


Fig. 3 Structure drawing of task management subsystem

is modified. When the system is started, the task information is detected. If there are uncompleted tasks, task management subsystem is called to continue execution of unfinished work.

3.4 Self-protection subsystem

In Android platform, there are three ways to realize the goal of destroying application programs, mandatory stop, uninstallation and clearing data. Three program destructive modes are shown in Fig. 4. These three states shall be, respectively, coped.

The adopted method is redundancy process. By generating two processes and using the communication between these two, life conditions between them are perceived. If one process is detected destroyed, corresponding measures are taken to protect mobile phones. To deal with the destruction of clearing data, data synchronization needs to be made between master–slave programs to prevent the data of one process from clearing. According to different data types and data synchronization modes, data types are divided into two types, system data and remote control record data.

4 Performance test and analysis

Performance test, respectively, tests the start-up time-consuming, CPU occupation, memory occupation, SMS task execution time of the system and the former three tests are carried out under Testin cloud test platform. A total of 150 real phones of different brands and series were used for tests. The installation, operation and uninstallation of them are shown in Table 2. SMS task execution time is executed on Samsung Galaxy Nexus.

Table 2 indicates that under normal conditions this system can be normally installed, operated and uninstalled on different Android mobile devices, with good adaptability.

4.1 Test results and analysis of start-up time-consuming

Start-up time-consuming refers to the consumed time of standup operation on mobile devices after the software is successfully installed and it is an important indicator of mobile phone application performance.

The test results of the system's start-up time-consuming are shown in Table 3.

The test result analysis of start-up time-consuming is shown in Fig. 5. The number of equipment within 2 s accounted for over 96 % of the total number of equipment. The minimum start-up time is only 0.32 s.

4.2 Test results and analysis of CPU occupation

CPU occupation refers to the occupied CPU time percentage in the system operation, and it is an important indicator of mobile phone application performance. The test results of CPU occupation are shown in Table 4.

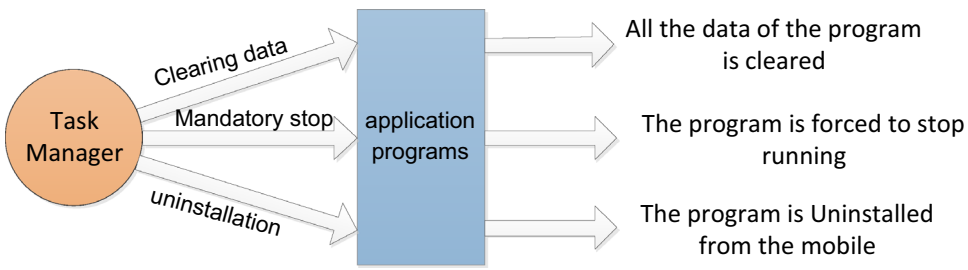


Fig. 4 Schematic diagram of three program destructive modes

Table 2 Test results table of the system installation, operation and uninstallation

Installation test				Start-up operation test				Uninstallation test			
	Number	Percentage	Passing rate (%)		Number	Percentage	Passing rate (%)		Number	Percentage	Passing rate (%)
Pass	146	97.3	100.0	Pass	141	94.0	96.6	Pass	141	94.0	100.0
Not pass	0	0.0		Not pass	5	3.3		Not pass	0	0.0	
Not executed	4	2.7		Not executed	4	2.7		Not executed	9	6.0	

Table 3 Test results of start-up time-consuming

Intervals (s)	0.29–0.93	0.94–1.57	1.58–2.21	2.22–2.85	2.86–3.47
Number	113	26	4	0	1
Percentage	78.5	18.1	2.8	0.0	0.7

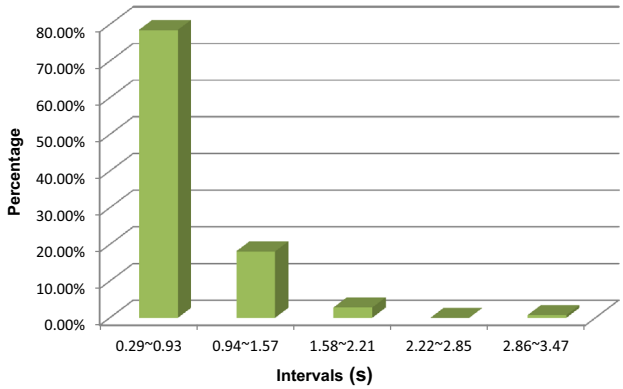


Fig. 5 Result analysis chart of start-up time-consuming test

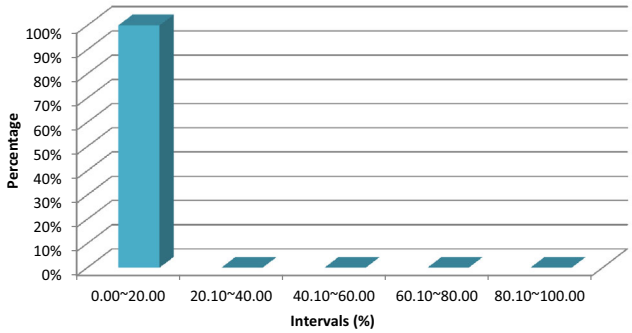


Fig. 6 Test result analysis chart of CPU occupation

The test result analysis of CPU occupation is shown in Fig. 6. CPU occupation of the system on all the test equipment is within 20 %, and the minimum CPU occupation only accounts for 0.35 %.

4.3 Test results and analysis of memory occupation

Memory occupation refers to the mobile phone ROM usage of the system. Same as CPU, this index also is an important evaluation indicator of mobile phone application performance. The test results of memory occupation are shown in Table 5.

The test result analysis of memory occupation is shown in Fig. 7. In the system operation, over 94 % equipment occupies less than 30 M.

4.4 Test results and analysis of SMS task execution time

This index is formulated according to this system. According to the non-functional requirements of the system, the mean time from sending instruction commands to receiving feedback SMS shall be no more than 5 min. Task execution adopts multi-thread technology to execute all the tasks in parallel. Thus, the execution time of command SMS depends on the task with the longest consumed time as long as the execution time of all tasks is no more than 5 min.

Tests are made on Galaxy Nexus equipment. Nine command SMSs were, respectively, sent, representing nine tasks, recording the sending time of SMS and the receiving time of feedback SMS. In this way, consumed time can be calculated. The mean of the test results is shown in Table 6. Figure 8 shows the histogram of the test results.

Test results indicate that the mean of task execution time is no more than 4 min, completely satisfying the non-functional requirements.

The test results of start-up time-consuming, CPU occupation, memory occupation and SMS task execution demonstrate that the performances of this system are good and do not occupy too much mobile phone resources, satisfying the requirements of normal mobile phone use.

5 Conclusion

This paper completed Android-based mobile phone privacy information protection system. Through the test of 150 real phones, it is found that the start-up time is within 2 s, CPU and memory occupation are reasonable, the mean of SMS task execution time is less than 4 min and the flow of 200 contact backing up is about 10 k. These indexes all satisfy the non-functional requirements of the system.

Table 4 Test results of CPU occupation

Intervals (%)	0.00–20.00	20.10–40.00	40.10–60.00	60.10–80.00	80.10–100.00
Number	145	0	0	0	0
Percentage	100	0	0	0	0

Table 5 Test results of memory occupation

Interval (MB)	0.00–16.02	16.03–32.04	32.05–48.06	48.07–64.08	64.09–80.12
Number	110	27	5	2	1
Percentage	75.9	18.6	3.4	1.4	0.7

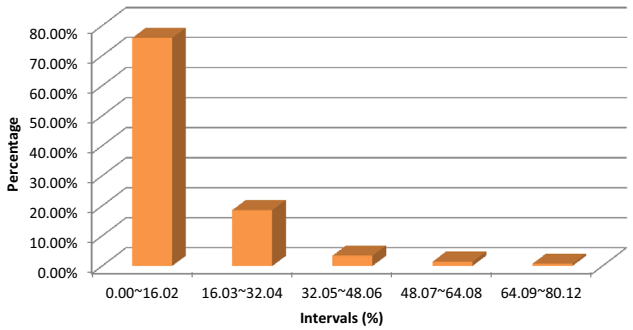


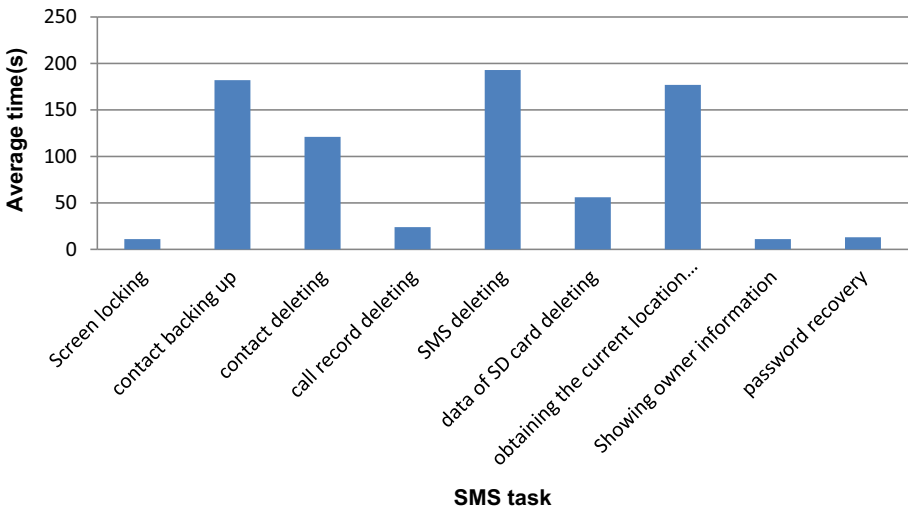
Fig. 7 Test result analysis chart of memory occupation

Table 6 Mean of SMS task execution time

SMS task	Scale	Time (s)
Screen locking	0	11
Contact backing up	200	182
Contact deleting	200	121
Call record deleting	100	24
SMS deleting	500	193
Data of SD card deleting	2 GB	56
Obtaining the current location of mobile phones	0	177
Showing owner information	0	11
Password recovery	0	13

Compared with the current mobile phone information protection software or measures, this system owns many innovations, mainly including the following aspects. (1) SMS remote control. The system does not hinder the normal use of mobile phones, and it does not execute unless it receives command SMS. It utilizes the most basic function of mobile phones to realize the mobile phone information protection. The operation is simple. (2) Dual-mode switch. To improve the user authority, the task manager of Android can delete any third party program, which can effectively hinder the virus Trojan propagation to certain level. However, it also may be hidden danger of the normal work of this system. Thus, this paper designed two modes. Under protection mode, Android process protection mechanism is used to prevent users from disturbing the system work. (3) Trusted number mechanism. Most mobile phone information protection software in market adopts C/S architecture, which saves password in server. When users forget codes, they can find password through server. This is troublesome and may own certain potential risks. This paper started from the view of users, setting trusted numbers for password recovery and executing some destructive operations. (4) Mail-contact backup. In the market, information backup software mostly backs up to the server of service providers, who may leakage user privacy. e-mail is one of the best services for user privacy protection, so it is convenient and safe to back up contact through it.

Fig. 8 Test result analysis chart of SMS task execution time



In future, mobile phone privacy information protection system based on Android will be implemented in Apple IOS platform. Also, Android-based virus detection system can be integrated into information protection system soon.

Acknowledgments This work is supported by the National Key Research and Development Program of China under grant No. 2016YFB0800801, the National Science Foundation of China (NSFC) under grant No. 61672186, 61472108, and the Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 20132302110037.

References

1. Wei T-E, Jeng AB, Lee H-M, Chen C-H, Tien C-W (2012) Android privacy. In: 2012 international conference on machine learning and cybernetics (ICMLC), vol 5. IEEE, pp 1830–1837
2. Vincent Messina (2012) Android4.0: lock screen 101. http://www.cultofandroid.com/10247/android-4-0-lock-screen-101/. 2012-5-7
3. Enck W, Ongtang M, McDaniel P (2009) Understanding android security. IEEE Secur Priv 1:50–57
4. Chiang H-S, Tsaur W-J (2010) Mobile malware behavioral analysis and preventive strategy using ontology. In: 2010 IEEE second international conference on social computing (SocialCom). IEEE, pp 1080–1085
5. Alazab M, Moonsamy V, Batten L, Lantz P, Tian R (2012) Analysis of malicious and benign android applications. In 2012 32nd international conference on distributed computing systems workshops (ICDCSW). IEEE, pp 608–616
6. Zhou Y, Jiang X (2012) Dissecting android malware: characterization and evolution. In: 2012 IEEE symposium on security and privacy (SP). IEEE, pp 95–109
7. Adeel M, Tokarchuk LN (2011) Analysis of mobile p2p malware detection framework through cabir & commwarrior families. In: 2011 IEEE third international conference on privacy, security, risk and trust (PASSAT) and 2011 IEEE third international conference on social computing (SocialCom). IEEE, pp 1335–1343
8. Schmidt AD, Bye R, Schmidt H-G, Clausen J, Kiraz O, Yüksel KA, Camtepe SA, Albayrak S (2009) Static analysis of executables for collaborative malware detection on android. In: IEEE international conference on communications, 2009. ICC'09. IEEE, pp 1–5
9. Bläsing T, Batyuk L, Schmidt A-D, Camtepe SA, Albayrak S (2010) An android application sandbox system for suspicious software detection. In: 2010 5th international conference on Malicious and unwanted software (MALWARE). IEEE, pp 55–62
10. Burguera I, Zurutuza U, Nadjm-Tehrani S (2011) Crowdroid: behavior-based malware detection system for android. In: Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices. ACM, pp 15–26
11. Shabtai A, Kanonov U, Elovici Y, Glezer C, Weiss Y (2012) "Andromaly": a behavioral malware detection framework for android devices. J Intell Inf Syst 38(1):161–190
12. Di Cerbo F, Girardello A, Michahelles F, Voronkova S (2010) Detection of malicious applications on android os. In: Computational forensics. Springer, Berlin, pp 138–149
13. Shakya N (2012) Privacy issues of antivirus apps for smartphones. In: The 12th winona computer science undergraduate research symposium, p 17
14. Liu J, Yu J (2011) Research on development of android applications. In: 2011 fourth international conference on intelligent networks and intelligent systems. IEEE, pp 69–72
15. Zhang D, Zhang D, Xiong H, Hsu C-H, Vasilakos AV (2014) BASA: building mobile ad-hoc social networks on top of android. IEEE Netw 28(1):4–9
16. Wang Y, Vasilakos AV, Jin Q, Ma J (2014) Survey on mobile social networking in proximity (MSNP): approaches, challenges and architecture. Wirel Netw 20(6):1295–1311
17. Zhou J, Cao Z, Dong X, Lin X, Vasilakos AV (2013) Securing m-healthcare social networks: challenges, countermeasures and future directions. IEEE Wirel Commun 20(4):12–21
18. Xia F, Liu L, Li J, Ma J, Vasilakos AV (2015) Socially aware networking: a survey. IEEE Syst J 9(3):904–921
19. Zhou J, Cao Z, Dong X, Xiong N, Vasilakos AV (2015) 4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf Sci 314:255–276
20. Xia F, Hsu C-H, Liu X, Liu H, Ding F, Zhang W (2015) The power of smartphones. Multimed Syst 21(1):87–101
21. Zhang W, Zhang Y, Kim T-H (2014) Detecting bad information in mobile wireless networks based on the wireless application protocol. Computing 96(9):855–874
22. Zhang W, He H, Zhang Q, Kim T (2014) PhoneProtector: protecting user privacy on the android-based mobile platform. Int J Distrib Sensor Netw 2014:10, Art ID 282417. doi:10.1155/2014/282417